МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«30» 08 2024 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«30» 08 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Безпека комп'ютерних мереж»
ступінь вищої освіти - бакалавр
галузь знань - 12 Інформаційні технології
спеціальність – 124 Системний аналіз
освітньо-професійна програма – Системний аналіз

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	ІРС (год.)	Тренінг (год)	СРС (год.)	Разом (год.)	Екзамен (сем)
ДФН	3	6	46	44	5	12	133	240	6

Тернопіль - 2024

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 - «Інформаційні технології» за спеціальністю 124 - «Системний аналіз», затвердженої Вченою радою ЗУНУ, протокол № 9 від 15.06.2022 р, зі змінами (протокол N11 від 26.06.2024 р.)

Робочу програму склав: д.т.н., професор, завідувач кафедри кібербезпеки Василь Яцків

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 124 «Системний аналіз», протокол №1 від 30.08.2024 р.

Голова групи
забезпечення спеціальності Роман ПАСІЧНИК

Гарант ОП Роман ПАСІЧНИК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ»

1. Опис дисципліни «Безпека комп'ютерних мереж»

Дисципліна «Безпека комп'ютерних мереж»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 8	Галузь знань 12 «Інформаційні технології»	Статус дисципліни – обов'язкова Мова навчання – українська
Кількість залікових модулів – 5	Спеціальність 125 «Системний аналіз»	Рік підготовки: 3 Семестр: 6
Кількість змістових модулів – 3	Ступінь вищої освіти – бакалавр	Лекції – 46 год. Лабораторні заняття – 44 год.
Загальна кількість годин – 240		Самостійна робота – 133 год. Тренінг – 12 год. Індивідуальна робота – 5 год.
Тижневих годин – 12, з них аудиторних – 6		Вид підсумкового контролю – іспит

2. Мета й завдання вивчення дисципліни «Безпека комп'ютерних мереж»

2.1. Мета завдання дисципліни

Мета вивчення дисципліни «Безпека комп'ютерних мереж» полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення безпеки комп'ютерних мереж, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту як окремих вузлів, так і комп'ютерної мережі в цілому, від зовнішнього та внутрішнього втручання.

Вивчення курсу «Безпека комп'ютерних мереж» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів (Основи програмування, WEB- технології, Операційні системи), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.2. Завдання вивчення дисципліни

В результаті вивчення курсу «Безпека комп'ютерних мереж» студенти повинні:

– засвоїти основні фундаментальні поняття і принципи побудови безпеки комп'ютерних мереж для їх використання в сучасних інформаційних системах;

– знати принципи побудови брандмауерів та фільтруючих маршрутизаторів і їх використання в задачах захисту інформаційних систем;

– використовувати методи для протидії від внутрішнього та зовнішнього втручання в професійній діяльності;

– вміти використовувати програмні засоби, які реалізують функції безпеки комп'ютерних мереж;

– програмно реалізовувати скрипти для конфігурування та забезпечення типових задач захисту інформації в комп'ютерних мережах;

– проектувати різні рівні захисту в вузлах та комп'ютерних мережах;

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

К02. Здатність застосовувати знання у практичних ситуаціях.

К04. Знання та розуміння предметної області та розумінняпрофесійної діяльності.

К05. Здатність спілкуватися державною мовою усно і письмово.

К06. Здатність спілкуватися іноземною мовою.

К15. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку,верховенства права, прав і свобод людини і громадянства України.

К17. Здатність використовувати системний аналіз як сучасну міждисциплінарну методологію, що базується на прикладних математичних методах та сучасних інформаційних технологіях і орієнтована на вирішення задач аналізу і синтезу технічних, економічних, соціальних, екологічних та інших складних систем.

К22. Здатність до комп'ютерної реалізації математичних моделей реальних систем і процесів; проектувати, застосовувати і супроводжувати програмні засоби моделювання, прийняття рішень, оптимізації, обробки інформації, інтелектуального аналізу даних.

К23. Здатність використовувати сучасні інформаційні технології для комп'ютерної реалізації математичних моделей та прогнозування поведінки конкретних систем а саме: об'єктно-орієнтований підхід при проектуванні складних систем різної природи, прикладні математичні пакети, застосування баз даних і знань.

К24. Здатність організовувати роботу з аналізу та проектування складних систем, створення відповідних інформаційних технологій та програмного забезпечення.

2.4 Результати навчання:

ПР13. Проектувати, реалізовувати, тестувати, впроваджувати, супроводжувати, експлуатувати програмні засоби роботи з даними і знаннями в комп'ютерних системах і мережах.

3. Програма навчальної дисципліни «Безпека комп'ютерних мереж»

Змістовий модуль 1. Безпека глобальних мереж та серверів

Тема 1. Основи безпеки Internet.

Internet і безпека. Організація IANA, RIR, LIR, AS та захист розподілу IP-адрес. Кореневі DNS та правила розподілу і функціонування доменних імен. Безпека рівнів TCP/IP. Захист на рівнях моделі відкритих систем OSI/ISO.

Тема 2. Стандарти, групи та класи захисту комп'ютерних мереж.

Стандарти оцінювання захисту. Критерії оцінювання захищених комп'ютерних систем Міністерства оборони США (TCSEC). Європейські критерії безпеки інформаційних технологій (ITSEC). Федеральні критерії безпеки інформаційних технологій США (FCITS). ISO/IEC 15408 "Common Criteria". Нормативні документи системи технічного захисту інформації України.

Тема 3. Рівні безпеки комп'ютерних мереж.

Законодавчий рівень. Адміністративний рівень. Засоби безпеки процедурного рівня. Засоби безпеки технічного рівня. Політики безпеки.

Тема 4. Безпека операційних систем серверів та мейнфремів.

Еволюція безпеки ОС (UNIVAC, CTTS, ITSS, Atlas, VMS, THE, RS4000, DOS). Захист в сімействі Windows (3.1, NT, 95, OS/2, 98, ME, 2000, XP, 2003, Vista, 7, 2008, 2012, 2016, 10, 2020). Безпека Unix-подібних ОС (AIX, HP-UX, IRIX, SCO-UX, SunOS, Solaris, BSD, FreeBSD, Linux). Засоби захисту сімейства MAC-OS. Операційні системи мейнфреймів та безпека (B5000, IBM System/360, UNIVAC 1108).

Тема 5. Основи захисту серверів ОС Windows.

Аутентифікація користувачів в серверах ОС Windows. Доступ на основі ресурсів серверів ОС Windows Управління доступом в операційних системах Windows на основі Active Directory. Централізовані системи аутентифікації і авторизації LDAP.

Тема 6. Засоби захисту UNIX-подібних систем (зокрема, Linux).

Аутентифікація в ОС сімейства Unix. Права груп і користувачів до файлів. Концепція єдиного логічного входу NIS. Система LDAP. Система Kerberos. Протокол SSH.

Змістовий модуль 2. Безпека інфраструктури та IP-мереж

Тема 7. Безпека фізичного рівня та кабельної інфраструктури.

Захист консольного доступу пристроїв та комп'ютерів. Безпека кабелів на основі міді. Волоконнооптичні кабелі та їх безпека. Захист в бездротових комп'ютерних мережах Wi-Fi. Захист мобільного зв'язку. Супутниковий зв'язок і його безпека. Пасивне мережеве обладнання.

Тема 8. Безпека канального рівня.

Активне мережеве обладнання і його захист. Повторювачі (Repeater). Концентратори (Hub). Мости (Bridge). Комутатори (Switch). Точки доступу (Access Point). Шлюз (Gateway). Фільтрація мережевих кадрів. Сегментація фізичних мереж. ARP-spoofing. Віртуальні локальні мережі VLAN. Протокол PPPoE. Віртуальні канали MPLS.

Тема 9. Фільтрація і моніторинг IP-трафіку.

Фільтрація. Види фільтрації. Стандартні і додаткові правила фільтрації маршрутизаторів. Типи фаєрволів. Фільтруючі маршрутизатори. Брандмауери та екрани. Пристрої UTM. Апаратні файєрволи. IDP-сигнатури атак. Системи детектування атак.

Тема 10. Поняття трансляції IP-адрес NAT.

Технологія NAT. Технологія SAT, PAT та Masqurade. IP-адреси для внутрішнього використання intarnet. Базова трансляція IP-адрес. Трансляція мережевих портів. Фаєрволи з функцією NAT. Програмні фаєрволи хоста.

Тема 11. Проксі-сервери.

Поняття кешуючих серверів. Проксі-сервери Лінукс. Проксі-сервери Віндовс. Наскрізний transparent-proxy. Конфігурування кешуючих серверів.

Тема 12. ICMP та IP– атаки мережевого рівня.

ICMP-атаки. Перенаправлення трафіку. ICMP-атака Smurf. ICMP-затоплення. Пінг смерті і ping-затоплення. Echo/chargen-затоплення. IP-атаки. Атака на IP-опції. IP-атака на фрагментацію.

Тема 13. Атаки на протоколи граничної маршрутизації.

Безпека маршрутизації на основі BGP. Уразливості і інциденти протоколу BGP. Маніпуляції з маршрутними оголошеннями. Захист BGP. Захист BGP-маршрутизації на основі бази даних маршрутів. Сертифікати ресурсів і їх використання для захисту BGP.

Змістовий модуль 3. Захист транспортних з'єднань та прикладних служб

Тема 14. Атаки на транспортний та сеансовий рівні TCP/ UDP.

UDP-атаки. UDP-затоплення. TCP-атаки. Затоплення SYN-пакетами Підробка TCP-сегмента. Скидання TCP-з'єднання.

Тема 15. Безпека протоколів прикладного рівня.

Протоколи HTTP, FTP, SMTP, POP3, IMAP4v1, SNMP, Telnet. Протокол передачі гіпертексту HTTP. Протокол передачі файлів FTP. Простий протокол передачі пошти SMTP.

Протокол отримання електронної пошти POP3. Протокол доступу до повідомлень мережі Інтернет IMAP4v1. Спам. Простий протокол керування мережевими пристроями SNMP. Протокол віддаленого доступу Telnet.

Тема 16. Сертифікати SSL та безпечні прикладні протоколи SSH і HTTPS.

Характеристики протоколу SSL. Ієрархія ключів та сертифікатів. Цифровий підпис даних в мережі. Протокол віддаленого доступу SSH. Протокол передачі гіпертексту HTTPS.

Тема 17. Атаки на доменні імена.

Атаки на DNS. DNS-спуффінг. Отруєння кеша DNS. Атаки на кореневі DNS-сервери. DDoS-атаки відображенням від DNS-серверів. Методи захисту служби DNS.

Тема 18. Сканери мереж.

Сканування мережі. Сканування портів. Виявлення мережевих сервісів та їх версій. Мережева розвідка. Виявлення версії операційної системи пристрою чи комп'ютера. Атаки на мережеві сервіси протоколів прикладного рівня. Сканер NMAP.

Тема 19. Моніторинг та виявлення атак.

Моніторинг трафіку. Аналізатори протоколів. Система моніторингу NetFlow та JFlow. Системи виявлення вторгнень. Система SNORTD. Архітектура мережі з захистом периметра. Мережі із поділом внутрішніх зон.

Тема 20. Віртуальні приватні мережі VPN.

Способи створення захищеного каналу. Транспортний і тунельний режими. Ієрархія технологій захищеного каналу. VPN на основі шифрування. Протокол PPTP. Розподіл функцій між протоколами IPSec. Український стандарт симетричного шифрування «Калина». Світовий стандарт симетричного шифрування AES.

4. Структура залікового кредиту дисципліни „Безпека комп'ютерних мереж"

	Кількість годин					
	Лекції	Лабораторні заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Безпека глобальних мереж та серверів						
Тема 1. Основи безпеки Internet.	2	2	4	1	2	Поточне опитування
Тема 2. Стандарти та групи та класи захисту комп'ютерних мереж.	2	2	6			
Тема 3. Рівні безпеки комп'ютерних мереж.	2	2	6			
Тема 4. Безпека операційних систем серверів та мейнфремів.	2	2	6			
Тема 5. Основи захисту серверів ОС Windows.	2	2	6			
Тема 6. Засоби захисту UNIX-подібних систем (зокрема, Linux).	2	2	6			
Змістовий модуль 2. Безпека інфраструктури та IP-мереж						

Тема 7. Безпека фізичного рівня та кабельної інфраструктури.	2	2	6	1	5	Поточне опиту-вання
Тема 8. Безпека канального рівня.	2	2	6			
Тема 9. Фільтрація і моніторинг IP-трафіку.	2	2	6			
Тема 10. Поняття трансляції IP-адрес NAT.	2	2	6			
Тема 11. Проксі-сервери.	2	2	6			
Тема 12. ICMP та IP–атаки мережевого рівня.	2	2	6			
Тема 13. Атаки на протоколи граничної маршрутизації.	2	2	6			
Змістовий модуль 3. Захист транспортних з'єднань та прикладних служб						
Тема 14. Атаки на транспортний та сеансовий рівні TCP/ UDP.	2	2	7	3	5	Поточне опиту-вання
Тема 15. Безпека протоколів прикладного рівня.	3	2	7			
Тема 16. Сертифікати SSL та безпечні прикладні протоколи SSH і HTTPS.	3	2	7			
Тема 17. Атаки на доменні імена.	3	3	9			
Тема 18. Сканери мереж.	3	3	9			
Тема 19. Моніторинг та виявлення атак.	3	3	9			
Тема 20. Віртуальні приватні мережі VPN.	3	3	9			
Разом	46	44	133	5	12	

5. Тематика лабораторних занять

Лабораторне заняття №1

Тема: Вивчення та дослідження приналежності IP-адреси
Мета: Вивчити та дослідити технологію видачі реальних IP-адрес
Питання для обговорення:

1. IANA
2. RIPE
3. ARIN
4. AfriNIC
5. APNIC
6. LANIC

Лабораторне заняття № 2

Тема: Видача доменних імен та їх безпека
Мета: Вивчити та дослідити принцип видачі імен в Інтернет

Питання для обговорення:

1. ДНС
2. Кореневі сервера
3. Кешуючі кореневі сервера ДНС
4. Зони ДНС
5. Зона UA
6. Зони COM і NET

Лабораторне заняття №3

Тема: Безпека серверів ОС Windows

Мета: Вивчити та дослідити принципи безпеки ОС Windows

Питання для обговорення:

1. Структура безпеки ОС Windows. Її переваги та недоліки.
2. Active Directory.
3. LDAP

Лабораторне заняття №4

Тема: Захист систем ОС Linux

Мета: Вивчення та дослідження захисту в ОС Linux

Питання для обговорення:

4. UNIX безпека
5. Linux безпека
6. Доступ до файлів
7. Права користувачів
8. Групи користувачі
9. NIS

Лабораторне заняття №5

Тема: Система фільтрації трафіку

Мета: Вивчити та дослідити **с**истеми фільтрації трафіку

Питання для обговорення:

1. Фільтруючий маршрутизатор
2. Iptables команда
3. Iptables таблиця
4. Таблиці фільтрації вхідного трафіку INPUT
5. Таблиці фільтрації вихідного трафіку OUTPUT
6. Таблиці фільтрації прохідного трафіку FORWARD

Лабораторне заняття № 6

Тема: Трансляція IP-адрес NAT.

Мета: Вивчити та дослідити принципи трансляції IP-адрес NAT.

Питання для обговорення:

1. Трансляціz трафіку NAT
2. Таблиці трансляції трафіку PREROUTING
3. Таблиці трансляції трафіку POSTROUTING
4. Таблиці трансляції трафіку MASQURADE

Лабораторне заняття № 7

Тема: Проксі-сервер
Мета: Вивчення та дослідження проксі-серверів
Питання для обговорення:

5. Проксі-сервера UNIX
6. Проксі-сервера Windows
7. Проксі-сервер Squid
8. Прості проксі-сервера

6. Самостійна робота

Самостійна робота з курсу «Безпека комп'ютерних мереж» виконується самостійно студентом на основі сформованого завдання, що охоплює основні теми курсу. Метою виконання самостійної роботи є дослідження та оволодіння навиками безпеки комп'ютерних мереж та серверів. Кожному студенту пропонується написання і представлення реферату на одну запропоновану або самостійно вибрану тему.

Орієнтовна тематика рефератів:

1. Модель загроз для операційної системи.
2. Типова архітектура комплексу засобів захисту операційних систем.
3. Порівняльна характеристика підходів до побудови захищених систем.
4. Критерії оцінювання захищених комп'ютерних систем Міністерства оборони США (TCSEC).
5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ).
6. Стандарт ISO 15408: основні документи, структура профілю захисту і завдання з безпеки.
7. Стандарт ISO 15408: структура стандарту, основні документи, структура вимог
8. Компоненти КЗЗ ОС Windows. Взаємодія компонентів і БД системи безпеки.
9. Підсистема розмежування доступу ОС Windows. Суб'єкти і об'єкти доступу.
10. Суб'єкти і об'єкти доступу ОС Windows. Реалізація дискреційного керування доступом.
11. Алгоритми з'ясування прав доступу в ОС Windows.
12. Реалізація підсистеми ідентифікації й автентифікації в ОС Windows.
13. Архітектура і модель безпеки системи UNIX. Основні недоліки традиційної моделі безпеки UNIX.
14. Підсистема ідентифікації та автентифікації UNIX. Підсистема розмежування доступу
15. PAM-автентифікація в Linux.
16. Реалізація мандатного керування доступом і адміністрування безпеки у середовищі Trusted Solaris
17. Security Enhanced Linux: політики, контексти безпеки, операції.
18. Процесори Intel i386: структури даних, що пов'язані з розмежуванням доступу до оперативної пам'яті.
19. Процесори Intel i386: реалізація кілець захисту; привілейовані і чутливі команди.
20. Процесори Intel i386: керування доступом до сегментів пам'яті під час звернень до нового сегмента та звернень за адресою у поточному сегменті.
21. Процесори Intel i386: керування викликом процедур і задач.
22. Загрози безпеці інформації у комп'ютерних мережах, віддалені атаки.
23. ITU-T, рекомендації X.800. Основні сервіси і механізми безпеки в мережах.
24. Проблеми протоколу IP і його реалізацій з точки зору безпеки інформації. Основні атаки на IP.
25. Проблеми протоколу TCP і його реалізацій з точки зору безпеки інформації. Основні атаки на TCP.
26. Безпека DNS. Можливі атаки.

27. Протокол ICMP. Можливі атаки. Рекомендації із застосування.

28. Проблеми протоколів Telnet і FTP. Уразливості. Методи захисту.

29. Безпека системи електронної пошти.

30. Безпека служби WWW: вразливості клієнтського ПЗ. Підвищення ступеня захищеності клієнтського ПЗ.

31. Безпека служби WWW: вразливості серверного ПЗ. Приклади атак.

32. Безпека CGI-застосунків: ін'єкції, методи захисту.

33. Міжмережні екрани. Класифікація, можливості й обмеження.

34. Віртуальні приватні мережі (VPN). Сервіси віртуальних приватних мереж. Типи віртуальних приватних мереж.

35. VPN віддаленого доступу. Протоколи PPTP і L2TP.

36. VPN мережного рівня. IPsec (протоколи, режими, утворення захищених асоціацій).

37. VPN сеансового рівня: функції посередництва, протоколи.

38. Засоби виявлення атак і протидії атакам.

Виконання самостійної роботи є одним із обов'язкових складових модулів залікового кредиту.

7. Тренінг з дисципліни

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання двох вибраних завдань тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Тематика тренінгу: Налаштування основних параметрів пристрою.

Орієнтовний перелік завдань для тренінгу:

1. Атаки в віртуальному середовищі.
2. Технології віртуалізації.
3. Мережеві загрози у віртуальному середовищі.
4. Захист віртуального середовища..
5. Схема захисту Deep Security.
6. Захист веб-додатків.
7. Розмежування прав.
8. Обмеження управління і політики.
9. Віртуальні загрози майбутнього.
10. Організація захисту від вірусів. Способи виявлення вірусів.
11. Проблеми антивірусів. Архітектура антивірусного захисту.
12. Боротьба з небажаною поштою
13. Міжмережеві екрани. Принципи роботи міжмережевих екранів.
14. Апаратні та програмні МЕ. Спеціальні МЕ.
15. Канали витоку.
16. Засоби запобігання витокам.
17. Засоби виявлення і запобігання вторгнень.
18. Промислові рішення моніторингу подій.

8. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни "Безпека комп'ютерних мереж" використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;

– підсумковий модульний контроль за кожним змістовним модулем;

– оцінювання виконання лабораторних робіт;

– оцінювання тренінгів;
– оцінювання результатів самостійної роботи;
– підсумковий письмовий екзамен.

9. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Безпека комп'ютерних мереж» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-11.	Підсумкова письмова робота за темами №1-13.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №12-22.	Підсумкова письмова робота за темами №14-20.	Визначається як середнє арифметичне з оцінок за виконання двох вибраних завдань тренінгу.	Визначається як середнє арифметичне за завдання самостійної роботи.	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання:

За шкалою університету	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов'язковим повторним курсом)

10. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Електронний варіант лекцій	1 -20
2	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1 - 20
3	Доступ до комп'ютерної мережі. Програмне забезпечення: Ocunetix, Nmap, Metasploit, Wireshark, John the Ripper, SQLninja, Cisco packet tracer 8.0.	1-20

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Курс мережевої академії Cisco: Network Security. Режим доступу https://www.netacad.com/courses/cybersecurity/network-security
2. Яцків В.В. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Безпека комп'ютерних мереж» для студентів галузі знань 12 Інформаційні технології, спеціальності 124 Системний аналіз, денної та заочної форм навчання. Тернопіль: ЗУНУ. 2024. 44 с.
3. Яцків В.В. Конспект лекцій з дисципліни «Безпека комп'ютерних мереж» для студентів галузі знань 12 Інформаційні технології, спеціальності 124 Системний аналіз, денної та заочної форм навчання. Тернопіль: ЗУНУ. 2024. 90 с.
4. Яцків В.В. Методичні рекомендації до виконання самостійної робіт з дисципліни «Безпека комп'ютерних мереж» для студентів галузі знань 12 Інформаційні технології, спеціальності 124 Системний аналіз, денної та заочної форм навчання. Тернопіль: ЗУНУ. 2024. 22 с.

Додаткова література

5. Jason Callaway. COMPUTER NETWORKING: 2 BOOKS IN 1 – All You Need to Know to Become a Networking Engineer from Scratch (Wireless Technologies, Network System, IP subnetting, Cybersecurity, and much more) - (October 8, 2021), 181 pages.
6. Scott Jernigan, Mike Meyers. CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008) 8th Edition - (March 28, 2022), 976 pages.
7. Craig Berg. Cisco Networking Essentials: Complete Guide To Computer Networking For Beginners And Intermediates (Code tutorials) Paperback – June 15, 2020, 85 pages.Larry L. Peterson, Bruce S. Davie. Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking) 6th Edition- (March 29, 2021), 848 pages.
8. José Manuel Ortega. Mastering Python for Networking and Security: Leverage the scripts and libraries of Python version 3.7 and beyond to overcome networking and security issues, 2nd Edition - (January 4, 2021), 538 pages.
9. Yatskiv V., Tsavolyk T., Yatskiv N., Koval V., Ivasiev S. Algorithm and data encoding/decoding devices based on two-dimensional modular correction codes. Proceedings of the 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2023), Khmelnytskyi, Ukraine, March 22–24, 2023, Vol-3373, 2023, ISSN 1613-0073. – Pp. 388-400. https://ceur-ws.org/Vol-3373/paper25.pdf
10. Yatskiv V., Nyemkova E., Kulyna S., Kulyna H., Ivasiev S. Data Encryption Method Based on the Redundant Residue Number System. Proceedings of the 5th International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, Khmelnytskyi, Ukraine, March 28, 2024, Vol-3675, 2024. – Pp. 223-235. [URL: https://ceur-ws.org/Vol-3675/paper16.pdf]